The defendant claimed that the search of his computers exceeded the scope of the warrant because no effort was made to first examine the files or directories that by their name or nature might indicate some type of record or list. Nor was any attempt made to ascertain whether the files at issue contained graphic, data base, spread sheet or word processing product.

In ruling, the court relied on the particularity requirement of the Fourth Amendment, as interpreted in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), which held that a warrant authorizing the search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity. Here, the warrant and supporting affidavit made clear the warrants authorized a search of the computers for documentary evidence relating to the defendant's illegal cable box operation. There was no ambiguity in the labeling of the "Fake I.D." folder; it clearly indicated that it probably contained false identification documents rather than records of the sale of illegal cable boxes. Mere inspection of the folder name gave the detective probable cause to seek a further warrant authorizing a search of the Sony computer for evidence of possession of forged instruments. Moreover, since the name extenders of the files in the Fake I.D. folder made it likely they contained images, it was unlikely they were text files sought by the warrant. Finally, the state's reliance on the plain view doctrine was misplaced, since none of the image files containing false identification documents was inadvertently discovered.

Third-Party Liability

Crime Prevention

Hard Drives as Criminal Instrumentalities?

Companies that discard computer hard drives without first making sure that sensitive customer or employee information has been removed risk contributing to crimes such as identity theft.

Despite a lack of case law, privacy and security experts agree that protection of such information is becoming an important issue, particularly in light of recent security breaches. Since January, there have been at least two major lawsuits involving stolen hard drives.

Moreover, a study from the Massachusetts Institute of Technology demonstrates the ease with which hard drives can be turned into instruments of crime. The study by two MIT students was based on an analysis of more than 150 hard drives, purchased mainly through eBay auctions. After several months of work and "relatively little financial expenditure," the students reported finding thousands of credit card numbers and "extraordinarily personal information on many individuals." One hard drive appeared to be used in an ATM machine.

"We believe that the lack of media reports about this problem is simply because, at this point, few people are looking to repurposed hard drives for confidential material," the students wrote.

Cases cropping up

Some recent cases suggest that the public already may be discovering how easy it is for hard drives with sensitive data to get into the wrong hands.

In January, a class-action lawsuit was filed in the U.S. District Court for the District of Arizona on behalf of 562,000 active and retired military personnel whose personal information was stolen late last year from a government contractor (*Stollenwerk v. TriWest Health Care Alliance Corp.*, D. Ariz., No. 2:03cv00185, *filed* 1/28/03).

The lawsuit claims that the contractor, TriWest Health Care Alliance Corp., was negligent under Arizona law by failing to protect individual privacy interests. It also alleges TriWest violated the Privacy Act of 1974.

According to a TriWest spokesman, the information was contained in hard drives from network servers that were stolen during a burglary of the firm's secondary buildings.

In another case, Canada's first ever privacy-related class action lawsuit, based on the theft of a computer hard drive containing personal information on more than 850,000 Canadians, was filed Feb. 3 (*Taylor v. Saskatchewan*, Sask. Q.B., No. 243, *filed* 2/3/03).

Culture change will reduce liability

Computer security training and procedures are key to reducing liability for mishandled hard drives, according to experts.

"The culture really has to change from top down," said Raymond J. Gustini, a partner with Nixon Peabody, in Washington. "I think companies have to recognize that this is not an overhead problem. It's a very important, fundamental business protection issue."

Experts advise companies to have an information security program in place that keeps track of personal data

they collect and vulnerabilities they are exposed to—electronically and physically, internally and externally. In addition, someone should be put in charge of overseeing the effectiveness of the program. Finally, organizations should also have a back-up plan to respond to information security problems.

Mark McLaughlin, president of Los Angeles-based Computer Forensics International, said companies must pay particular attention to hard drives when it comes to computer security.

"I think it's an area that people pretty much forget about," McLaughlin said. "A lot of emphasis is put on the Web as far as security, but not here. With increased personal identity theft, permanently deleting data should be a priority." In a recent report, the Federal Trade Commission said that identity theft complaints lodged in its Consumer Sentinel database doubled from 86,198 in 2001 to 161,819 in 2002.

Prevention

McLaughlin and other experts say the best way to remove information from a hard drive is to overwrite data multiple times.

However, Technology Recycling recommends destroying hard drives.

This method "provides the highest degree of certainty that companies are protecting their data and maintaining compliance with new federal privacy laws," the firm said in a white paper released last November.

Both methods—overwriting data and destroying hard drives—are included in security standards developed by the Department of Defense.

The Defense Department's standards on cleaning hard drives can be found in its "National Industrial Security Program Operating Manual," available at http://www.dss.mil/isec/nispom_0195.htm. Technology Recycling's "White Paper on Corporate Computer Disposal Issues" is available at http://www.techrecycle.com/.

Cyberstalking

Third-Party Liability May Attach to Information Brokers

Liability may attach to a web-based investigation and information service that sold personal information about a young woman to a man who then tracked her down at work and murdered her, the New Hampshire Supreme Court held Feb. 18. (*Remsburg v. Docusearch Inc.*, 2003 WL 346260 N.H. (2/18/03).

Responding to questions certified by a federal court, Justice Linda S. Dalianis said that a private investigator or information broker (such as a credit reporting agency) has a duty to exercise reasonable care toward third parties whose Social Security numbers it sells to clients. She further found that a third party whose Social Security number is sold without knowledge or permission may have a cause of action for intrusion upon seclusion against the seller, and that obtaining a person's work address through a pretextual phone call and selling it violates the state's Consumer Protection Act.

"We think this is the first court to rule as a matter of law that information brokers can be liable for the foreseeable harm that flows from the sale of personal information," such as Social Security numbers, said Chris J. Hoofnagle, an attorney with the Electronic Privacy Information Center who filed an amicus brief in the case.

Amy Lynn Boyer was shot and killed in 1999 at her workplace by Liam Youens, who then shot and killed himself. Youens obtained Boyer's Social Security number, home address, and work address by purchasing the information from Docusearch Inc. Docusearch obtained the Social Security number from a credit reporting agency as part of a credit report. A Docusearch subcontractor obtained Boyer's work address by placing a "pretext" telephone call to her in which the subcontractor lied about who she was and the purpose of her call in order to convince Boyer to disclose her employment information.

After Boyer's murder, her mother sued Docusearch and the subcontractor.

Duty of care owed

The court first considered whether a private investigator or information broker who sells information to a client pertaining to a third party has a legal duty to the third party, under New Hampshire common law, with respect to the sale of the information. It said that a "private citizen has no general duty to protect others from the criminal attacks of third parties." However, an exception to that rule may arise when there is an "especial temptation and opportunity for criminal misconduct brought about by the defendant."

The court observed that identity theft "is an increasingly common risk associated with the disclosure of personal information" and carries severe consequences for victims. Another crime linked to disclosure of personal information is stalking, which causes serious psychological harm to victims and has been criminalized in all 50 states, the court said.

"The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client," the court said. "This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information," it added.

David A. Gottesman, Gottesman & Hollis, Nashua, N.H., argued for the mother. Andrew R. Schulman, Getman, Stacey, Tamposi, Schulthess & Steere, Bedford, N.H., argued for Docusearch.